UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/578,767	03/22/2007	**David Spooner**	042933/386648	6135

826 7590 08/18/2010

ALSTON & BIRD LLP
BANK OF AMERICA PLAZA
101 SOUTH TRYON STREET, SUITE 4000
CHARLOTTE, NC 28280-4000

EXAMINER	
WRIGHT, BRYAN F	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
08/18/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/578,767	SPOONER, DAVID	
	Examiner	Art Unit	
	BRYAN WRIGHT	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *3/22/2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 May 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *5/5/2006, 10/20/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to original filings on 5/5/2006. Claims 1-39 are pending.

Priority

Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d).

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1, 3-6 are rejected under 35 U.S.C. 102(e) as being anticipated by Hind et al. (US Patent No. 6,980,660 and Hind hereafter).

3. As to claim 1, Hind teaches a method of controlling access to a specific resource on a mobile telephone (i.e., ..teaches and a method of discrete (i.e. per device, per user, per group, per application, or per transaction) access control, including the ability

to add, revoke or change access privileges in a mobile environment (e.g., mobile phone) [col. 7, lines 30-40]).; comprising the steps of:

(a) associating an identity with a permission state (i.e., ...teaches based on the contents of the verified certificate of the first device, can consult a local or enterprise access control database using the required device identifier or optional (associated individual or group names) certificate fields to decide what resources/functions may be exercised via the encrypted connection [col. 11, lines 45-60]), in which an identity (e.g., device identifier) is a label applicable to one of several entities (e.g., device) on whose behalf the resource could potentially be used (e.g., exercised) and the permission state defines whether or not the resource can actually be used (i.e., teaches an access control database at a server, the certificates provide a method of controlling access to services and resources, as well as selecting preferences which should be enabled for the device [col. 11, lines 65-67 and col. 12, lines 1-5]);

and (b) allowing use (e.g., exercise) of the resource solely to an entity or entities labeled with an identity associated with a permission state that does permit such use (i.e., ...teaches based on the contents of the verified certificate of the first device, can consult a local or enterprise access control database using the required device identifier or optional (associated individual or group names) certificate fields to decide what resources/functions may be exercised via the encrypted connection [col. 11, lines 45-60]).

4. As to claim 3, Hind teaches a method in which the permission state (e.g., preference) includes a permission type and a value (i.e., ...teaches electing preferences which should be enabled for the device, such as formatting a data stream for a specific type of display or enabling access to specific data records [col. 11, lines 65-67 and col. 12, lines 1-5]).

5. As to claim 4, Hind teaches a method in which a permission state associated with a given identity can be updated or altered (i.e., ..teaches including the ability to add, revoke or change access privileges [col. 7, lines 35-38]).

6. As to claim 5, Hind teaches a method in which the updating or alteration of a permission state (e.g., access privileges) is done on instructions sent from a computer remote from the mobile telephone (i.e., ..teaches a method applicable to any mobile environment where devices are frequently accessing other devices to securely generate and exchange cryptographic keys which can be used for encryption and other purposes for discrete (i.e. per device, per user, per group, per application, or per transaction) access control, including the ability to add, revoke or change access privileges including the ability to add, revoke or change access privileges [col. 7, lines 30-40]).

7. As to claim 6, Hind teaches a method in which use of the resource includes one or more of: access, deployment, alteration or deletion (i.e., ...teaches based on the contents of the verified certificate of the first device, can consult a local or enterprise

access control database using the required device identifier or optional (associated individual or group names) certificate fields to decide what resources/functions may be exercised via the encrypted connection by 2003 [col. 11, lines 45-60] ...further teaches a method for discrete (i.e. per device, per user, per group, per application, or per transaction) access control, including the ability to add, revoke or change access privileges including the ability to add, revoke or change access privileges [col. 7, lines 30-40]).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2 and 7-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind in view of Proust et al. (US Patent No. 6,216,014 and Proust hereinafter (cited from IDS)).

8. As to claim 2, Hind teaches access control on a per application basis, however Hind does not expressly discloses: A method comprising the steps of (a) a script or other kind of executable code associated with a given entity sending a request to use the specific resource a computer program embodied on the machine; the script being labeled with an identity or including a secure signature from which an identity can be

deduced ; (b) a software component running on the device processing the request and using the identity to determine the applicable permission state associated with the identity for that script or executable code. However at the time of applicant's original filing, prior art reference Proust disclosed an application (e.g., script) running on a SIM module. See Proust abstract. Proust further disclosed that the application (e.g., script) identifiable by unique identifier (e.g., loyalty application). See Proust figure 4. The Examiner notes figure 4 of Proust further illustrates the operation of accessing a system resource (e.g. file) in a mobile environment and that the application (e.g., script) is a given an access control policy indicators. See Proust Figure 3B. The Examiner contends when an application attempts to access a file (e.g., resource), the policy information of that particular application making the access attempt is checked to determine if that application can access that file. Therefore to enhance the resource access control capability of Hind, a person with ordinary skill in the art would have recognized that such enhancement is rendered by modifying Hind's capability to provide access control on a per application basis with the capability disclosed by Proust to use policy data to determine if an application (e.g., script) can access a specific resource.

9. As to claim 7, Hind teaches access control on a per application basis, however Hind does not expressly discloses: A method in which the script or other kind of executable code associated with a given entity is labeled with an additional identity separate from or independent of the identity of the given entity, the additional label identifying the script or code. However at the time of applicant's original filing prior art

reference Proust disclosed utilizing application (e.g., script) identifiers such that the identifier would determine access privileges to system resource (e.g., file). See Proust figures 3B and figure 9. Therefore to enhance the resource access control capability of Hind, a person with ordinary skill in the art would have recognize that such enhancement is rendered by modifying Hind's capability to provide access control on a per application basis with the capability disclosed by Proust to used application identifier and resource identifiers to determine if an application (e.g., script) can access a specific resource.

10. As to claim 8, Hind teaches access control on a per application basis, however Hind does not expressly discloses: A method in which the component can use the permission state associated with the additional identity to enable it to determine if the script itself is permitted to use the resource, irrespective of whether the given entity is allowed to use the resource. However at the time of applicant's original filing prior art reference Proust disclosed utilizing access control policy to determine if an application (e.g., script) could access system resource (e.g., file). See Proust figures 3B and figure 9. Additionally, the Examiner notes Proust discloses the use of identifiers and the associated access privileges. Therefore to enhance the resource access control capability of Hind, a person with ordinary skill in the art would have recognize that such enhancement is rendered by modifying Hind's capability to provide access control on a per application basis with the capability disclosed by Proust to used application identifier

and resource identifiers to determine if an application (e.g., script) can access a specific resource.

11. As to claim 9, Hind teaches a method in which the script or code (e.g., access privileges) can have its identity altered (i.e., ..teaches including the ability to add, revoke or change access privileges [col. 7, lines 35-38]).

12. As to claim 10, Hind teaches a method in which the alteration is a result of instructions sent to the telephone from a remote computer (i.e., ..teaches a method applicable to any mobile environment where devices are frequently accessing other devices to securely generate and exchange cryptographic keys which can be used for encryption and other purposes for discrete (i.e. per device, per user, per group, per application, or per transaction) access control, including the ability to add, revoke or change access privileges including the ability to add, revoke or change access privileges [col. 7, lines 30-40]).

13. As to claim 11, Hind teaches access control on a per application basis, however Hind does not expressly discloses: A method of in which the identity is altered to an identity associated with a higher or broader permission state only if the script or code has been authenticated to a pre-defined confidence level. However at the time of applicant's original filing prior art reference Proust disclosed utilizing access control policies with different permission levels to determine if an application (e.g., script) could

access system resource (e.g., file). See Proust figures 3B and figure 9. Additionally, the Examiner notes Proust discloses the use of identifiers and the associated access privileges. Therefore to enhance the resource access control capability of Hind, a person with ordinary skill in the art would have recognize that such enhancement is rendered by modifying Hind's capability to provide access control on a per application basis with the capability disclosed by Proust to used application identifier and resource identifiers to determine if an application (e.g., script) can access a specific resource.

14. As to claim 12, Hind teaches a method in which the method is deployed on the mobile telephone by a component that is not part of the operating system and can therefore be installed onto the telephone without needing to be burnt into the main ROM of the telephone that stores the operating system (i.e., teaches the use of a mobile phone environment (e.g., SIM, memory, operating system [1003, fig. 1A]).

15. As to claim 13, Hind teaches a method in which the component runs in the secure SIM of the mobile telephone (i.e., teaches the use of a mobile phone environment (e.g., SIM, memory, operating system [1003, fig. 1A]).

16. As to claim 14, Hind teaches a method in which the permission states and their association with different identities are stored in the SIM, but the component runs outside the SIM (i.e., teaches the use of a mobile phone environment (e.g., SIM, memory, operating system [1003, fig. 1A]).

17. As to clam 15, Hind teaches a method of further comprising the step of remotely administering the permission states associated with different identities, by sending instructions from a computer remote from the computer (i.e., ..teaches an administer remote from the mobile phone environment possessing the capability to configure permission through instructions [col. 6, lines 5-25]).

18. As to claim 16, Hind teaches a method in which the component stores (e.g., access control debase) in memory, or accesses from memory a list of the permission states associated with different identities (e.g., device identities) (i.e., teaches an access control database at a server, the certificates provide a method of controlling access to services and resources, as well as selecting preferences which should be enabled for the device based on the device identifier [col. 11, lines 65-67 and col. 12, lines 1-5]).

19. As to claim 17, Hind teaches a method in which an identity is determined for any script (e.g., software on the device) that seeks to access code by an authentication process using a digital signature (col. 8, lines 25-30).

20. As to claim 18, Hind teaches a method of in which the authentication process generates an identity handle (e.g., device identifier) that can be transferred as a token (col. 10, lines 1-15].

21. As to claim 19, Hind teaches a method in which the identity handle has an associated confidence level based on the authentication (i.e., ...teaches based on the contents of the verified certificate of the first device, can consult a local or enterprise access control database using the required device identifier or optional (associated individual or group names) certificate fields to decide what resources/functions may be exercised via the encrypted connection by 2003 [col. 11, lines 45-60]).

22. As to claim 20, Hind teaches a method in which the entity is an individual end-user (e.g., ...teaches per user access control, including the ability to add, revoke or change access privileges [col. 7, lines 30-40]).

23. As to claim 21, Hind teaches a method in which the entity is a network operator (e.g., ...teaches per user access control, including the ability to add, revoke or change access privileges [col. 7, lines 30-40]).

24. As to claim 22, Hind teaches a method in which the entity is a mobile telephone manufacturer (e.g., ...teaches per user access control, including the ability to add, revoke or change access privileges [col. 7, lines 30-40]).

25. As to claim 23, Hind teaches a method in which the entity is an application developer or vendor (e.g., ...teaches per user access control, including the ability to add, revoke or change access privileges [col. 7, lines 30-40]).

26. As to claim 24, Hind teaches a method in which the entity is an employer (e.g., ...teaches per user access control, including the ability to add, revoke or change access privileges [col. 7, lines 30-40]).

27. As to claim 25, Hinds teaches a method in which the entity is an operation (e.g., teaches per transaction access control [col. 7, lines 30-40]).

28. As to claim 26, Hind teaches initialization (e.g., boot code) of a mobile however Hind does teach a method in which the operation is booting the telephone so that startup code is run, the startup code having a specific identity, and the permissions for this identity determine what can or cannot be done at startup. However at the time of applicant's original filing prior art reference Proust disclosed utilizing code (e.g., boot code) to render the appropriate operation performed on a mobile device. The code associated to control policies with different permission levels to determine if an application (e.g., script) could access system resource. See Proust figures 9 and figure 10. Additionally, the Examiner notes Proust discloses the use of identifiers and the associated access privileges. Therefore to enhance the resource access control capability of Hind, a person with ordinary skill in the art would have recognize that such enhancement is rendered by modifying Hind's capability to provide access control on a per application basis with the capability disclosed by Proust to used application identifier

and resource identifiers to determine if an application (e.g., script) can access a specific resource.

29. As to claim 27, Hind teaches a method in which the entity is an operation (e.g., transaction) of a timer going off (e.g., those skilled in the art would recognize that the transaction/operation will have a associated time duration) (i.e.., teaches per transaction access control [col. 7, lines 30-40]).

30. As to claim 28, Hind teaches a method in which the entity is a kind or type of entity (e.g., device) (i.e. per device, per user, per group, per application, or per transaction) access control, including the ability to add, revoke or change access privileges including the ability to add, revoke or change access privileges [col. 7, lines 30-40]).

31. As to claim 29, Hind teaches a method in which at least two entities (e.g., device group) do not have identities (e.g., device ids) that are associated with permission states (e.g., access control) that are hierarchically arranged with respect to each other (e.g., teaches per group access control [col. 7, lines 30-40]).

32. As to claim 30, Hind teaches a method in which no entities (e.g., devices) have identities (e.g., device ids) that are associated with permission states (e.g., access

control) that are hierarchically arranged with respect to each other (e.g., teaches per device access control [col. 7, lines 30-40]).

33. As to claim 31, Hind teaches a method in which no entity (e.g., device) automatically has rights to use all resources on the telephone (e.g., teaches per device, access control [col. 7, lines 30-40]).

34. As to claim 32, Hind teaches access control within a mobile environment however Hinds does not teach a method in which the resource is specific data. However at the time of applicant's original filing prior art reference Proust disclosed utilizing access control policies with different permission levels to determine if an application (e.g., script) could access a file (e.g., specific data). See Proust figures 3B and figure 9. Additionally, the Examiner notes Proust discloses the use of identifiers and the associated access privileges. Therefore to enhance the resource access control capability of Hind, a person with ordinary skill in the art would have recognize that such enhancement is rendered by modifying Hind's capability to provide access control on a per application basis with the capability disclosed by Proust to used application identifier and resource identifiers to determine if an application (e.g., script) can access a specific resource.

35. As to claim 33, Hind teaches a method in which the permission state determines whether the data can be read, modified or deleted (i.e. ...teaches access control, including the ability to add, revoke or change access privileges [col. 7, lines 30-40]).

36. As to claim 34, Hind teaches access control within a mobile environment however Hinds does not teach a method in which the resource is a specific executable application and the permission state determines whether the application can be run or updated However at the time of applicant's original filing prior art reference Proust disclosed utilizing access control policies with different permission levels to determine if an application (e.g., script) could access a file (e.g., executable application). See Proust figures 3B and figure 9. Additionally, the Examiner notes Proust discloses the use of identifiers and the associated access privileges. Therefore to enhance the resource access control capability of Hind, a person with ordinary skill in the art would have recognize that such enhancement is rendered by modifying Hind's capability to provide access control on a per application basis with the capability disclosed by Proust to used application identifier and resource identifiers to determine if an application (e.g., script) can access a specific resource.

37. As to claim 35, Hind teaches access control within a mobile environment however Hind does not teach a method in which the resource is a hardware resource on the telephone. However at the time of applicant's original filing prior art reference Proust disclosed utilizing access control policies with different permission levels to determine if

an application (e.g., script) could access a file (e.g., specific data). See Proust figures 3B and figure 9. Additionally, the Examiner notes Proust discloses the use of identifiers and the associated access privileges. Therefore to enhance the resource access control capability of Hind, a person with ordinary skill in the art would have recognize that such enhancement is rendered by modifying Hind's capability to provide access control on a per application basis with the capability disclosed by Proust to used application identifier and resource identifiers to determine if an application (e.g., script) can access a specific resource.

38. As to claim 36, Hind teaches access control within a mobile environment however Hind does not teach a method in which the resource is a networking or communications resource on the telephone. However at the time of applicant's original filing prior art reference Proust disclosed utilizing access control policies with different permission levels to determine if an application (e.g., script) could access a system resource (e.g., networking or communications resource). See Proust figures 3B and figure 9. Additionally, the Examiner notes Proust discloses the use of identifiers and the associated access privileges. Therefore to enhance the resource access control capability of Hind, a person with ordinary skill in the art would have recognize that such enhancement is rendered by modifying Hind's capability to provide access control on a per application basis with the capability disclosed by Proust to used application identifier and resource identifiers to determine if an application (e.g., script) can access a specific resource.

39. As to claim 37, Hind teaches a method n which the step of associating an identity (e.g., device id) with a permission state (e.g. optional data) results in a record of the association stored in a memory of the telephone (fig. 4).

40. As to claim 38, Hind teaches access control within a mobile environment however Hind does not teach a method in which the step of allowing use of the resource takes place by a CPU in the telephone processing data. However at the time of applicant's original filing prior art reference Proust disclosed utilizing access (e.g., allowing use) control policies with different permission levels to determine if an application (e.g., script) could access a system resource. See Proust figures 3B and figure 9. Additionally, the Examiner notes Proust discloses the use of identifiers and the associated access privileges. Therefore to enhance the resource access control capability of Hind, a person with ordinary skill in the art would have recognize that such enhancement is rendered by modifying Hind's capability to provide access control on a per application basis with the capability disclosed by Proust to used application identifier and resource identifiers to determine if an application (e.g., script) can access a specific resource.

41. As to claim 39, Hind teaches access control within a mobile environment however Hind does not teach a mobile telephone with specific resources, in which access to the resources is controlled. However at the time of applicant's original filing

prior art reference Proust disclosed utilizing access (e.g., allowing use) control policies with different permission levels to determine if an application (e.g., script) could access a system resource. See Proust figures 3B and figure 9. Additionally, the Examiner notes Proust discloses the use of identifiers and the associated access privileges. Therefore to enhance the resource access control capability of Hind, a person with ordinary skill in the art would have recognize that such enhancement is rendered by modifying Hind's capability to provide access control on a per application basis with the capability disclosed by Proust to used application identifier and resource identifiers to determine if an application (e.g., script) can access a specific resource.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/William R. Korzuch/
Supervisory Patent Examiner, Art Unit 2431